Amendments to the Claims

1.-22. (Canceled)

23. (New) A method for preserving the integrity of a negotiation conducted via a network, such as, the Internet, and using clients and/or servers, among a plurality of parties each of whom is making a private input during the negotiation and wherein a trusted entity acting as a center computes and outputs a value F of these inputs constituting the output of the negotiation comprising the steps of:

a) providing an architecture which includes a center A, and a plurality of participants B.sub.l, B.sub.2,..., B.sub.n, to engage in a negotiation during which all communications originating with a participant B.sub.i and transmitted to center A are exclusive;
b) secretly generating an input x.sub.i by each participant B.sub.i;
c) publishing by the center A to each participant a commitment to K combinatorial circuits that compute F, where K is a security parameter;
d) transmitting by each participant B.sub.i to the center A a commitment c.sub.i to the value of B.sub.i's input x.sub.i, where c.sub.i is an encryption of x.sub.i;
e) responsive to receipt of the commitments of the participants, publishing by the center A to the participants the commitments received;
f) providing to each participant B.sub.i part of the K combinatorial circuits that the center A committed to, and requesting center A to open them, whereupon each participant B.sub.i can verify that the part of the circuits opened to participant B.sub.i computes a value F;
g) transmitting by each participant B.sub.i to center A its input x.sub.i and decryption data to enable center A to verify that x.sub.i corresponds to the transmitted commitment c.sub.i;
h) computing by center A a value of F based on the inputs x.sub.i it received by using a part of the K combinatorial circuits not disclosed to the participants, and publishing the computed value of F to the participants; and
i) transmitting to all participants a proof that the computed value of F was computed correctly,

which proof can be verified by each participant using the published commitments while preventing a coalition of any one subset of participants from learning (i) anything which cannot be computed just from the output of the K combinatorial circuits and from their own inputs, and (ii) information about the inputs of other users.

24. (New) The method of claim 23 wherein step i is carried out using a value F' that is computed from the K combinatorial circuits using inputs x.sub.i and outputs j,Y of the computed value of F, F' outputs 1 if and only if X(j)=Y, and X(j)>=X(i) for every i different from j.

25. (New) The method of claim 23 wherein interaction between each participant and center A is carried out using a secure two-party function evaluation protocol run between each participant, B.sub.i and center A, the input of B.sub.i being a value x.sub.i and the input of center A being a description of a function f so that at the end of the protocol, B.sub.i learns f(x), but no other information about f, and center A learns nothing about x.sub.i, thereby, the input x.sub.i is a private input of B.sub.i, and the function f is a private input of center A.

26. (New) The method of claim 24 wherein the protocol is based on expressing *f* as a combinatorial circuit of gates over a preselected fixed base, and wherein the bits of the input are entered into input wires and are propagated through the gates so that a pseudo-random isomorphic transformation of the circuit is generated producing a "garbling" of the circuit.

27. (New) A method for preserving the integrity of a negotiation conducted via a network, such as, the Internet, and using clients and/or servers, among a plurality of parties each of whom is making a private input during the negotiation and wherein a trusted entity acting as a center computes and outputs a value F of these inputs constituting the output of the negotiation comprising the steps of:

a) announcing by center A that it will compute F;
b) providing an architecture which includes a center A, and a plurality of participants B.sub.l, B.sub.2,..., B.sub.n, to engage in a negotiation during which all communications

originating with a participant B.sub.i and transmitted to center A are exclusive;

c) constructing by center A K garbled circuits including gates having wire inputs and outputs that compute F;

d) choosing by center A a permutation of each wire input of the circuits;

e) publishing by center A to each participant B.sub.i tables of gates, and commitments to the permutations and the garbled values of the input wires;

f) secretly generating an input x.sub.i by each participant B.sub.i;

g) transmitting to center A, for every input wire for every circuit corresponding to an input bit known to participant B.sub.i, a commitment of the permuted value of the input bit;

h) responsive to receipt of the commitments of the participants, publishing by the center A to the participants the commitments received;

i) selecting by each participant B.sub.i a subset of the K garbled circuits that the center A committed to;

j) revealing by center A its commitments to the subset of the K garbled circuits, whereupon each participant B.sub.i can verify that the circuits revealed to participant B.sub.i computes value F;

k) verifying by participants that test circuits compute F;

l) transmitting by each participant B.sub.i to center A its input x.sub.i and decryption data to enable center A to verify that x.sub.i corresponds to the transmitted commitment in step g;

m) computing by center A a value of F based on the inputs x.sub.i it received by using circuits not in the subset disclosed to the participants, and publishing the computed value of F to the participants;

n) publishing by center A opened commitments and corresponding garbled inputs; and

o) transmitting to all participants a proof that the computed value of F was computed correctly, which proof can be verified by each participant using the published opened commitments and corresponding garbled inputs while preventing a coalition of any one subset of participants from learning (i) anything which cannot be computed just from the output of the K garbled circuits and from their own inputs, and (ii) information about the inputs of other users.

28. (New) The method of claim 27 including the further step of each participant submitting its input to a trusted third party who can open an input in the event a participant refuses to open its commitment in step l.

29. (New) The method of claim 27 including the further step of each participant being required to use an optional forced opening when making its commitment to its input thereby enabling center A to recover the committed value without the help of the participant making the commitment, if a participant is not willing to open the commitment.

30. (New) The method of claim 27 including the further step of requiring each participant to back up it commitment financially.

31. (New) A method for preserving the integrity of a transaction conducted via a network, such as, the Internet, and using clients and/or servers, among a plurality of parties each of whom is making a private input during the transaction and wherein a trusted entity acting as a center computes and outputs a value F of these inputs constituting the output of the transaction comprising the steps of:

a) providing an architecture which includes a center A, and a plurality of participants B.sub.l, B.sub.2,..., B.sub.n, to engage in a transaction during which all communications originating with a participant B.sub.i and transmitted to center A are exclusive;
b) secretly generating an input x.sub.i by each participant B.sub.i;
c) publishing by the center A to each participant a commitment to K secure circuits that compute F, where K is a security parameter;
d) transmitting by each participant B.sub.i to the center A a commitment c.sub.i to the value of B.sub.i's input x.sub.i, where c.sub.i is an encryption of x.sub.i;
e) responsive to receipt of the commitments of the participants, publishing by the center A to the participants the commitments received;
f) providing to each participant B.sub.i part of the K secure circuits that the center A committed to, and requesting center A to open them, whereupon each participant B.sub.i

can verify that the part of the circuits opened to participant B.sub.i computes a value F;

g) transmitting by each participant B.sub.i to center A its input x.sub.i and decryption data to enable center A to verify that x.sub.i corresponds to the transmitted commitment c.sub.i;

h) computing by center A a value of F based on the inputs x.sub.i it received by using a part of the K secure circuits not disclosed to the participants, and publishing the computed value of F to the participants; and

i) transmitting to all participants a proof that the computed value of F was computed correctly, which proof can be verified by each participant using the published commitments while preventing a coalition of any one subset of participants from learning (i) anything which cannot be computed just from the output of the K secure circuits and from their own inputs, and (ii) information about the inputs of other users.